2006 CCRTS
The State of the Art and the State of the Practice

Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability

Topics:
C2 Architectures
C2 Concepts and Organizations
Information Operations/Assurance

Author:
Christopher John Raney
SPAWAR Systems Center San Diego

Address:
53560 Hull Street
San Diego, CA 92152-5001

Phone/Fax:
619-553-5282 / 619-553-1114

E-Mail:
raneyc@spawar.navy.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Systems Center,53560 Hull Street,San Diego,CA,92152-5001**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**28**	

Abstract:

Information superiority, the capability to collect, process, and disseminate an uninterrupted flow of information, is the cornerstone of Command and Control (C2). With the increasing coalition and multinational aspects of warfare in the 21st century, we must extend key information to our allies and coalition partners to ensure shared information dominance. Traditional information sharing methods such as automated guards or a "man-in-the-loop" has well documented problems including data loss through the guards and operational picture integrity.

A multilevel C2 system has been developed and deployed that allows a multinational integrated operational picture to be maintained and disseminated by US Intelligence Analysts. This system leverages the capability of a trusted operating system by storing all data in labeled files and using the operating system to enforce access control. This approach is difficult to extend to a service oriented architecture (SOA) because SOA infrastructures are large, complex entities that are not multilevel.

In this paper, we address the issues associated with integrating an existing multilevel C2 system into a larger service oriented architecture. We present an architecture that can be generalized to integrate other MLS systems. We then propose a future architecture which addresses the limitations in the current system.

Introduction

Joint Vision 2010, the conceptual template for leveraging technology to provide effective capability to the joint warfighter, outlines the critical elements necessary to transform the DoD in to a superior force for the 21st century. Two of the elements necessary for this transformation are information superiority and multinational operations. In order to effectively realize Joint Vision 2010, we must provide the capability for U.S. forces to collect, process, and disseminate an uninterrupted flow of information with allied and coalition partners.

Two of the biggest challenges in interoperating with allied and coalition partners are those of disclosure and releasability. [Gause, Et Al] Often times we will have data that is useful to our partners, but we can not share it with them because it is classified inappropriately. With the current "system-high" command-and-control systems in use today, any data that we receive from our partners automatically "floats up" and becomes classified at the high watermark of the receiving system. Once the data is classified at this higher level, it cannot be released to our partners, even though the data was originally classified at a level releasable to them. The current system-high architecture effectively traps data that is otherwise releaseable.

Data which has been floated to a higher level must be either manually downgraded or sanitized via an automated system before it is releasable. Manual downgrade requires that one or two people review the data, which can be quite labor intensive if there is a large volume of data to release. Automated sanitization is another solution, but the automated sanitization process often modifies the original data and can therefore cause unnecessary loss of data and degradation of the data quality or precision. [Chang, Et Al.] Neither of these two solutions is ideal.

The ideal solution would be to provide a system that can automatically release appropriate data to allied and coalition partners without loss of information. By utilizing Multilevel Secure (MLS) labeled data stores that are accessible via the network, we can completely avoid the typical problems of disclosure and releasability in coalition warfare and thus provide automated data release of the data in its entirety.

Background on MLS

The DISA publication entitled "Multilevel Security in the Department of Defense" defines Multilevel Security as:

> *Multilevel security*, or *MLS*, is a capability that allows information with different sensitivities (i.e., classification and compartments) to be simultaneously stored and processed in an information system with users having different security clearances, authorizations, and needs to know, while preventing users from accessing information for which they are not cleared, do not have authorization, or do not have the need to know. MLS capabilities often can help overcome the

operational constraints imposed by system-high operations and can foster more effective operations.

The concept of MLS was originally devised in the 1960's by DoD to support missions which required the integration of data from multiple classification levels. DoD and private industry expended a significant amount of development effort on MLS technology beginning in the 1960's and continuing through the 1980's. Development on MLS technologies by industry slowed during the 1990's due to a number of issues including long development times, evaluation-time uncertainties, and application compatibility issues. [Saydjari]

Although industry development on MLS technology slowed, the DoD still had to find solutions to address the fact that military operations are inherently multilevel. Thus, the idea of the "guard" was born. A guard is a "processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a database to filter out data that the user is not authorized to access". [CNSS] Guards became the transfer mechanism of choice for passing data between security levels. Although guards made it easier to transfer data, they did so at a cost. The cost of transferring data through a guard comes either in terms of additional labor for a manual review process, or loss of data during an automated process.

In 1998, the United States Navy fielded the Joint Cross Domain eXchange, a multilevel C2 system based on an MLS trusted operating system. JCDX essentially alleviates the need for a sanitizer or guard since the data is kept in a labeled format such that the original security level is maintained and is therefore typically low enough to be releasable.

Background on the Joint Cross Domain eXchange (JCDX)

The Joint Cross Domain eXchange (JCDX) is an accredited protection-level-4 (PL4), operational, multi-level secure, command and control system. The JCDX multilevel system combines HP-UX workstations, a Trusted Operating System (TOS), Commercial and Government Off-the-Shelf (COTS/GOTS) components and JCDX application specific software to provide a highly capable and secure system. JCDX goes beyond providing an MLS system as it includes a rich set of intelligence data management and analysis features.

JCDX was designed to meet the original security and functional requirements of an older MLS system while transitioning the security architecture from an application based security model to an operating system based security model. The operating platform selected was HP 10.26 running on HP workstations because it provided the security foundation for a complex, modern system. The biggest payoff in converting to a commercial operating system has been the ability to incorporate commercial and GOTS software with little or no change to the JCDX system.

MLS systems such as JCDX have typically been reserved for use in highly specialized applications by a small number of users due to the accreditation costs and other issues associated with deploying MLS systems and their associated clients. In the network architecture envisioned by the Global Information Grid (GIG) systems will no longer require the use of dedicated clients but instead will be accessible to any client over the network. MLS systems must adapt and be accessible via the network as well. Integrating a Web Services interface on an MLS system such as JCDX extends the Mandatory Access Control (MAC) capabilities of an MLS operating system to users on non-MLS systems. In addition, providing a web services interface on existing MLS systems allows reuse of years of previous research and development and allows the extension of those capabilities to users and other systems on the Global Information Grid.

Recently JCDX underwent this transformation effort to develop a web services interface. The JCDX Web Services interface provides a mechanism for labeled data storage and cross domain data transfer capabilities to operate within a Service Oriented Architecture (SOA). By utilizing Multilevel Secure labeled data stores, which are accessible via the network to multiple coalition partners, the typical problems of disclosure and releasability can be completely avoided.

The integration of JCDX in to a Service Oriented Architecture

The Horizontal Fusion Portfolio Initiative was launched by the DoD Office of the Assistant Secretary of Defense for Networks Integration / Defense Chief Information Officer to accelerate the transition of Net-Centric Warfighting from vision to reality. The Horizontal Fusion Portfolio process invests in initiatives that are DoD programs of record, as well as promising emerging technologies, which can be accelerated to Net-Centric operation. Net-Centric Enterprise Services (NCES) supplies the infrastructure and services to support the broad range of applications and data used in Horizontal Fusion.

As part of the Horizontal Fusion (HF) effort, JCDX was identified to serve as the core data labeling technology to allow other HF portfolio participants to have access to data across multiple security domains in a transparent manner. For Horizontal Fusion, the JCDX team developed two web services, a Classification Policy Decision Service (cPDS), and a Federated Search Provider (FSP). The cPDS web service primarily provides other systems with methods for handling labeled data such as label comparison. The federated search provider allows users and applications to search multi-level data stores from single level networks and provides a “read down” capability to all lower level domains.

To provide defense-in-depth, cPDS and the Federated Search Provider are implemented on a separate server known as the JCDX Web Services Server (JWSS). The JWSS provides the web service interface to the JCDX server and a separate JWSS is currently required for each network on which web services are made available. Each JWSS operates at a single security level and has one dedicated network connection to the JCDX server and one to the attached network. (See Figure 1)

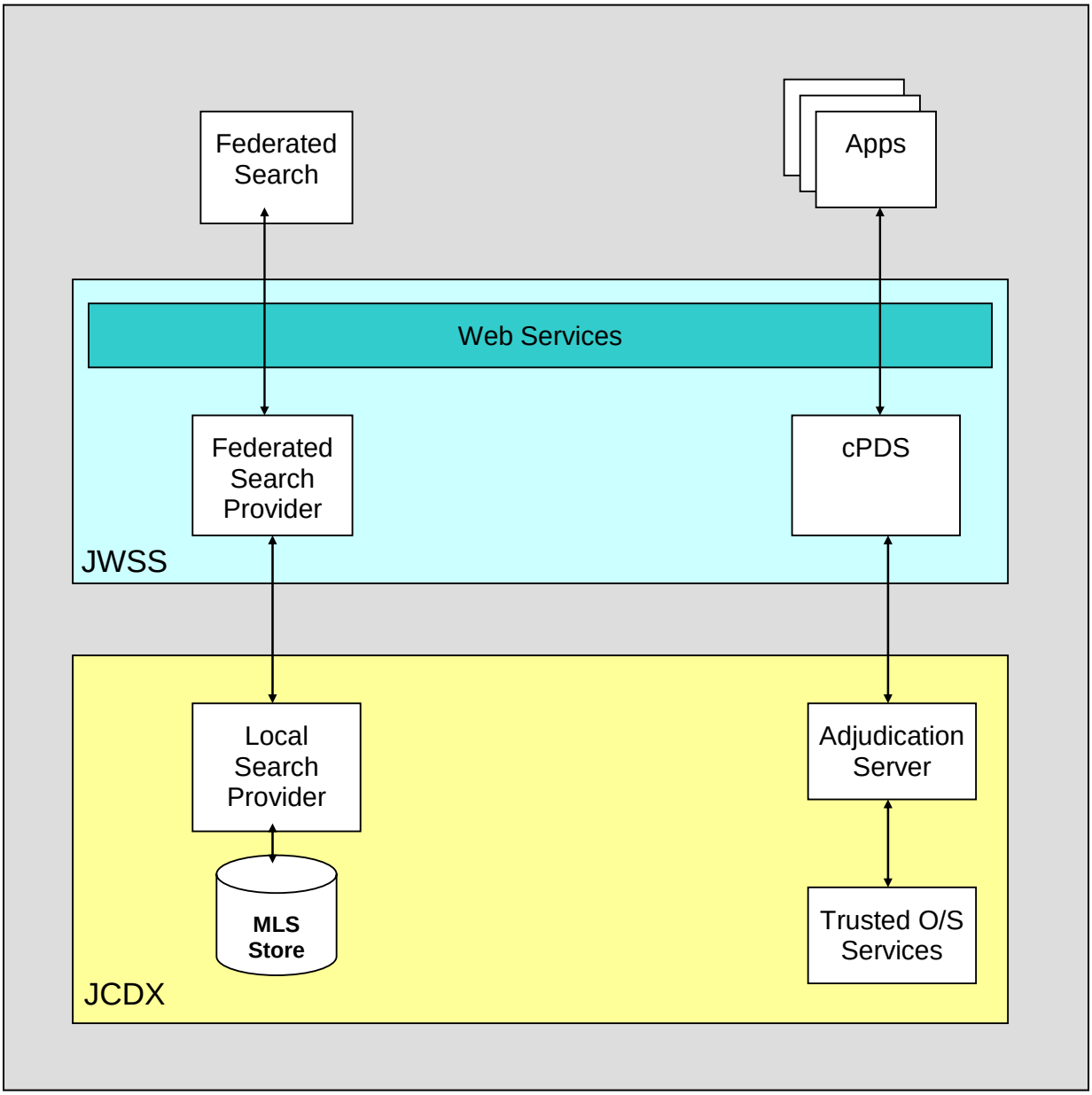


Figure 1: JCDX Web Services Architecture

The first step to enable other systems to handle labeled data was to extend the NCES Security Services to include clearance based mandatory access control (MAC). The current NCES Security Services implements role based access control but not clearance based access control. cPDS provides the capability of the JCDX MLS clearance based MAC policy through a web service. An example use of cPDS is a user authenticating to a web portal that requires a specific clearance level for access. The portal first attempts to authorize the user via NCES RBAC and then attempts to authorize the user's clearance via JCDX cPDS (See Figure 2).

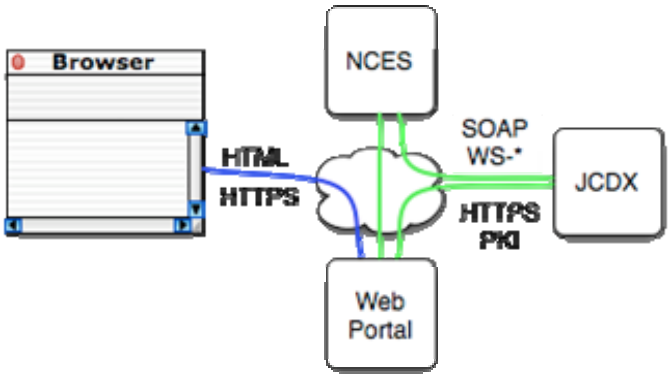


Figure 2: Web Portal Authorizing User's Role via NCES and User's Clearance via JCDX cPDS

cPDS is composed of three parts: Security Adjudication Web Service, cPDS Apache Axis Handler, and cPDS SDK. The Security Adjudication Web Service implements validity, comparison, and aggregation operations on Department of Defense Discovery Metadata Standard (DDMS) SecurityType labels. The cPDS Apache Axis Handler implements clearance based access control in conjunction with existing DISA or DIA NCES handlers. The cPDS SDK includes source code and test cases for implementing clearance based access control within applications.

cPDS provides a number of methods useful for handling labeled data including:

- **isValid:** The *isValid* method takes a classification and returns validation of the classification.
- **getRelationship:** The *getRelationship* method takes two arguments, a Subject Clearance and an Object Classification and returns the relationship between the two arguments. The relationship can be one of the following: Subject Strictly Dominates, Equal, Object Strictly Dominates, and Incomparable
- **getAggregateClassifcation:** The *getAggregateClassification* method takes a list of classifications and produces a 'sum' of the arguments" classification. The resulting classification is the clearance required to read the objects whose classifications were used as arguments (e.g. *getAggregateClassification* 'SECRET REL GBR' 'SECRET' 'UNCLASSIFIED' yields 'SECRET').
- **getGroupClearance:** The *getGroupClearance* method takes a list of user clearances and produces a group clearance. This group clearance is the highest classification that can be read by all users in the group (e.g. *getGroupClearance* 'TOP SECRET' 'SECRET REL GBR' 'CONFIDENTIAL' yields 'CONFIDENTIAL REL GBR').
- **iSReleasableTo:** The *isReleasableTo* method takes a data classification and a list of clearances and determines whether the data can be released to all users whose clearances were used as arguments.
- **canReceive:** The *canReceive* method takes a user clearance and a list of data classifications and determines whether the user can see all the data whose

classifications were used as arguments. The *canReceive* and *isReleasableTo* services can be implemented in terms of the *getRelationship*, *getAggregateClassification* and *getGroupClearance* services, but it is more convenient and efficient to call these methods directly.

The second web service developed for HF is JCDX's Federated Search Provider. The Federated Search Provider allows searching of the JCDX MLS PL4 data repository through a Web Service. The provider authenticates the search request via NCES and cPDS (See Figure 3) and then returns messages at the appropriate classification — including "read-down" — with search terms highlighted. The multilevel data stores that can be searched include raw and processed intelligence, track databases, and unformatted files such as text and PDF.

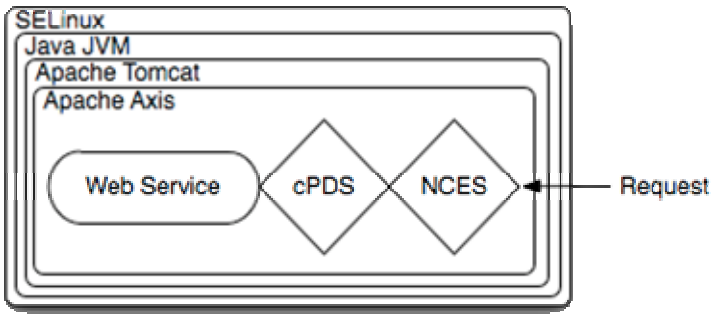


Figure 3: Requests to JCDX's Federated Search Provider must first be authorized via NCES and cPDS

Issues in current SOA and suggestions for the future

Although significant progress has been made in extending MLS services to SOA, there are a number of issues that must be solved before full MLS capability can be provided. In this section, we raise some of these issues and pose possible solutions.

The architecture that was developed for JCDX and presented in this paper addresses how users can "consume" content, but there are a number of issues associated with producing content as well. Content producers need a method to produce labeled content in which the label can be trusted with a high level of confidence. The most widely deployed client operating system, Microsoft Windows, is currently a platform with very little assurance. It is not reasonable to expect every user to have a full MLS system as their client machine. One possible solution for content producers that are on low assurance platforms is to utilize a high assurance editor to produce content that can be trusted and then transferred to the MLS service. Another possible solution is the use of a high assurance review mechanism that would require all data that is produced to be digitally signed by a designated reviewer.

In order to transfer labeled data there must be a trusted interaction between two systems. In the current non-SOA deployments, these trust relationships are statically defined. In a

network-centric deployment, the list of services to which a system communicates with will not necessarily be pre-defined. Since we cannot pre-define these trust relationships, we need an automated method to determine which services on the network are trusted. This leads to the concept that the network could have a central "trust" service. The trust service could be queried to determine the level of trust that a given service on the network possesses.

When using MLS systems, the issue of what mechanism should be used for labeling the data always arises. One possible labeling method that could be applied to multilevel SOA is that of a "labeling service". The labeling service would provide an interface to allow the submission of content for labeling. The labeling service would then assign a security label to the content based on a pre-defined ruleset. The labeling service would then "sign" the associated label to allow other services to verify the given label.

Another significant issue to overcome in achieving a full multilevel services oriented architecture is that of accreditation. An accreditation decision is granted based on the level of trust that can be given to a particular system. Some of the questions that arise when extending MLS to SOA include: "How do we put all of these individually trusted services together to produce a single trusted service?" and "Does the composition of many trusted services yield a single trusted service, or do we need some sort of trusted path?". Perhaps "trusted path" is no longer a valid concept in a SOA. Perhaps we should look at trusted transactions, to include the state of the transaction and the data in the transaction.

To achieve a full multilevel services oriented architecture these critical pieces must still be addressed. Some of the critical pieces such as the trusted editor, trusted review process, trust service, and labeling service can be addressed by technology development. The remaining issues of policy and accreditation will change at a much slower pace but will likely accelerate once the remaining pieces have been developed.

Conclusion

Over the past 40 years, DoD has expended a considerable amount of effort on cross domain solutions with most of the effort being focused on stovepipe systems that cannot interact with each other. JCDX has begun to bridge the gap between traditional MLS systems and SOA and has developed an architecture that can be applied to other MLS systems. By extending MLS systems to interoperate within a SOA, we are one step closer to achieving the ultimate goal of a single secure global multinational solution set enabling seamless sharing of information within multiple communities of interest to include our allied and coalition partners.

References

Kenneth Gause, Catherine Lea, Daniel Whiteneck, Eric Thompson. Center for Naval Analyses. U.S. Navy Interoperability with its High-End Allies. Avaialble Online at http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track3/080.pdf.

DISA, Multilevel Security in the Department Of Defense: The Basics. 1 March 1995

Chang, LiWu; Moskowitz, Ira. A Study of Inference Problems in Distributed Databases. Naval Research Laboratory. 2002. Available Online at http://www.chacs.itd.nrl.navy.mil/publications/CHACS/2002/2002chang-ifip02.pdf

Saydjari, O. Sami. Multilevel Security: Reprise. Security & Privacy Magazine, IEEE. Volume 2, Issue 5, Sept.-Oct. 2004 Page(s):64 – 67

Committee on National Security Systems (CNSS). NSTISSI Intstruction No. 4009. National Information Assurance Glossary, 2003; Available Online at http://www.nstissc.gov/assets/pdf/4009.pdf

Joint Cross Domain eXchange (JCDX): Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability

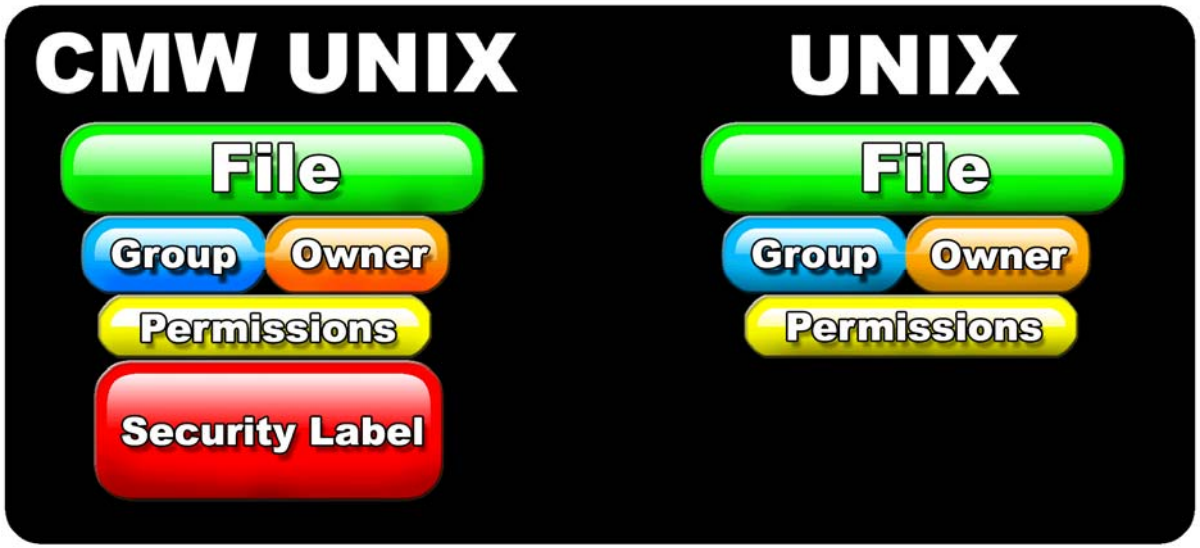
An Accredited Approach
to Cross Domain Information Sharing

Presented By:
Christopher J Raney
SSC San Diego

Multi-Level Secure (MLS)

- MLS labels every file at the appropriate security level
- Labeled files are only accessible to users with the proper security clearance

- The labeled files are compared to the user's credentials and proper access is only given to their appropriate level



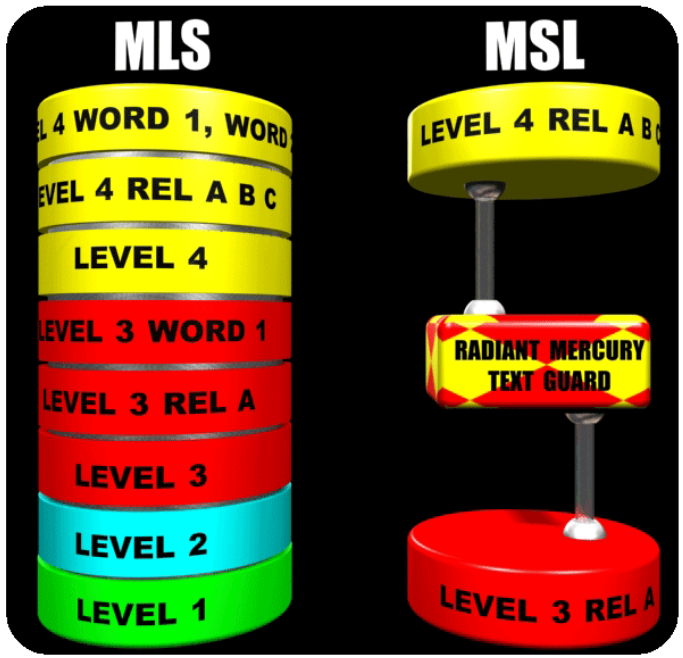
CMW:

Compartmented Mode Workstation. The core operating system of an MLS system.

Multiple Security Levels (MSL) Challenges

- Multiple Security Levels (MSL)
  - A conglomeration of single-level workstations/servers used to provide information for analysis.
  - Information is passed between the two systems utilizing security guards, which strips off valuable intelligence data from remarks lines.

- With an MLS solution such as JCDX, only a single system requires management. *MSL* environments require at a minimum, a separate system per security level.

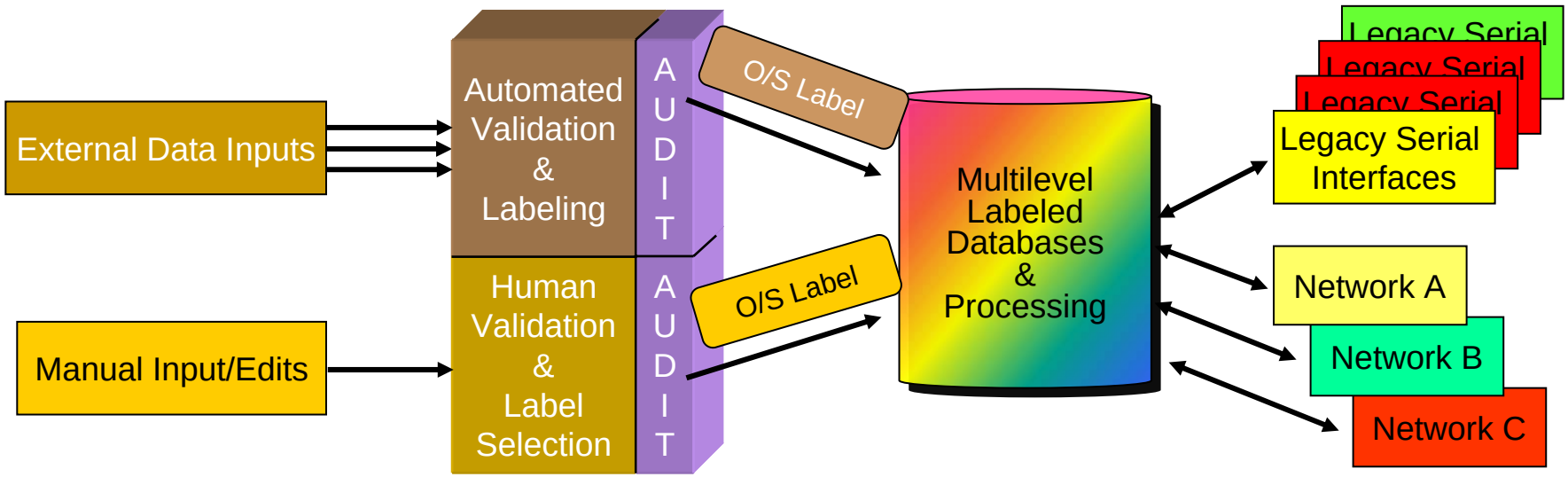


MSL should not be confused with MLS:

Multiple Security Levels are limited to separate application displays and downgrading of information can result in loss of valuable data.

What is JCDX today?

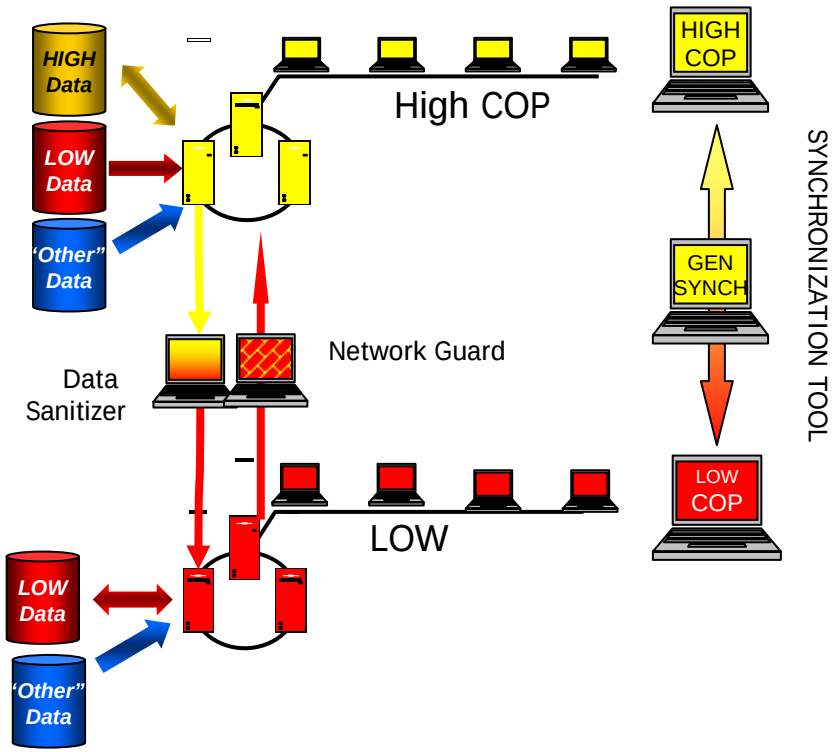
- A certified, operational, multi-level secure (MLS), PL4, all-source data management, display, fusion processing and near real-time dissemination capable system
- JCDX labels incoming data (tracks / messages / other products) from multiple sources / classification levels, manages that data (correlation, manipulation) and transmits data out to multiple sources at multiple classification levels



Cross Domain Solution Architectures

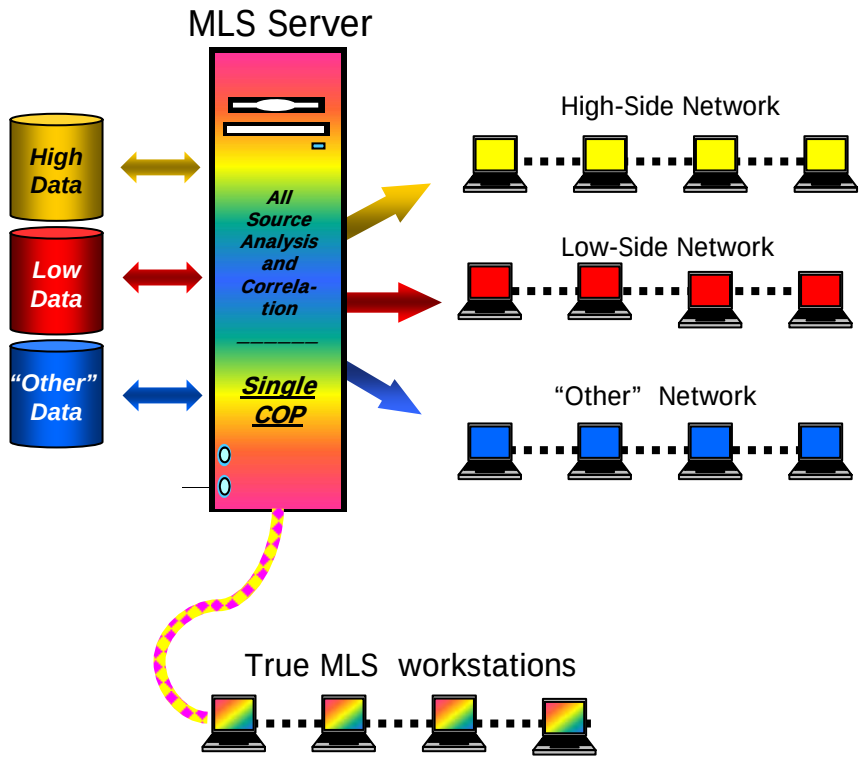
UNCLASSIFIED

Generic Architectures Today



Multiple Security Levels (MSL)

JCDX pre SOA

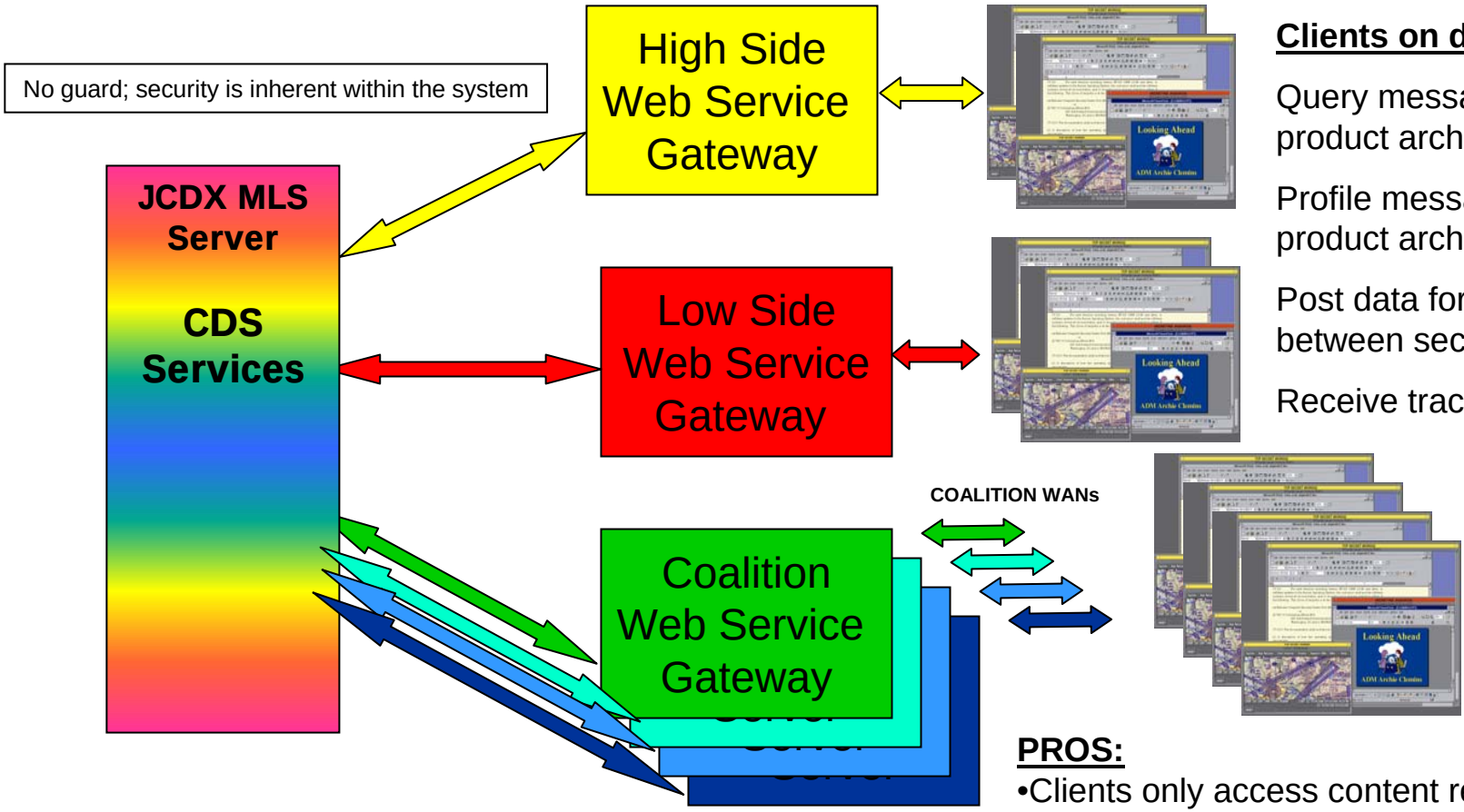


Multi-Level Security (MLS)

No guard; security is inherent within the system

UNCLASSIFIED

JCDX Architecture with SOA Extensions



Clients on different WANS:

Query message and intel product archive

Profile message and intel product archive for updates

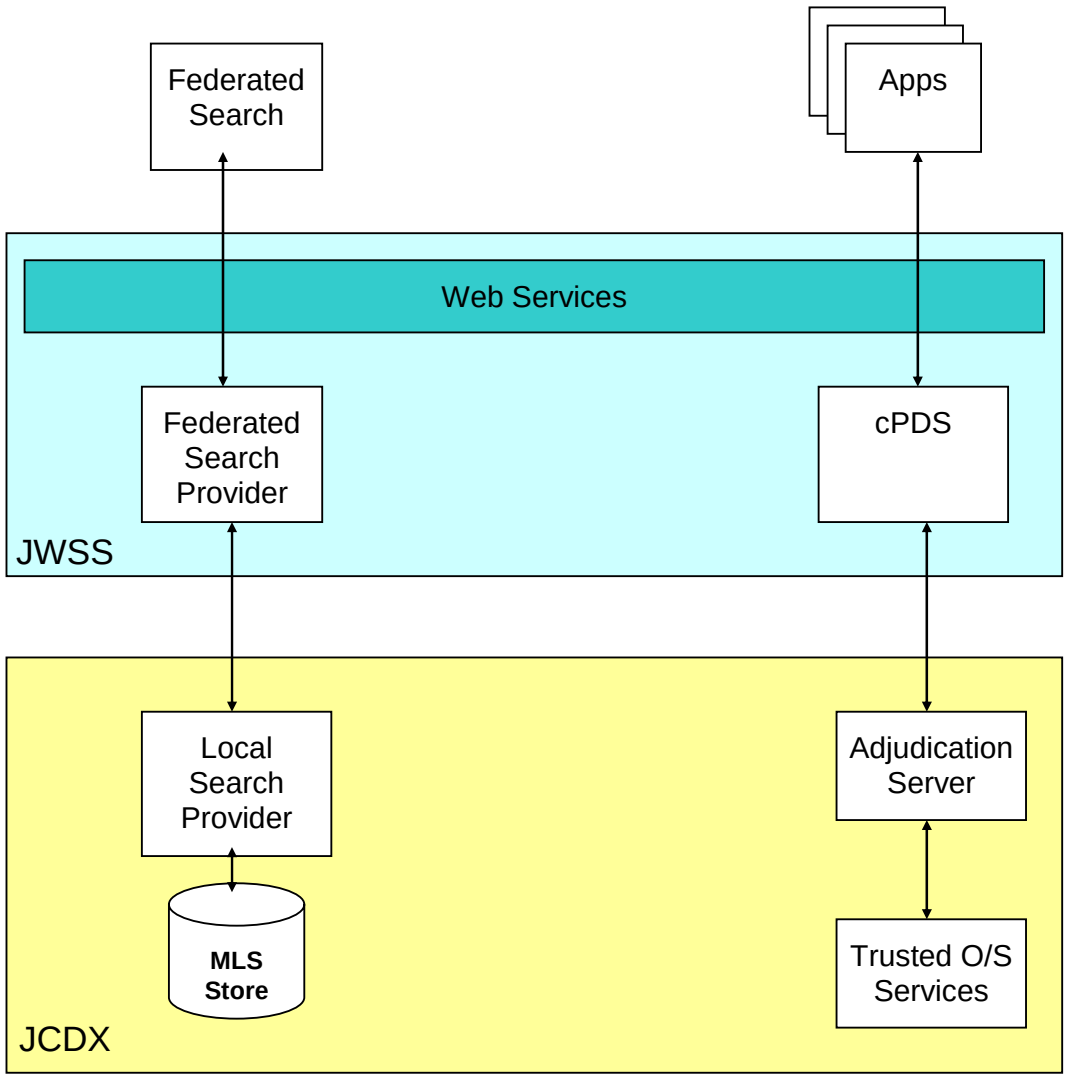
Post data for collaboration between security domains

Receive tracks for display

PROS:

- Clients only access content releasable to their domain (Mandatory Access Control)
- Data producers only need to "Post Once" for data to be available to all applicable domains
- No unnecessary data loss from sanitizers

SOA Architecture

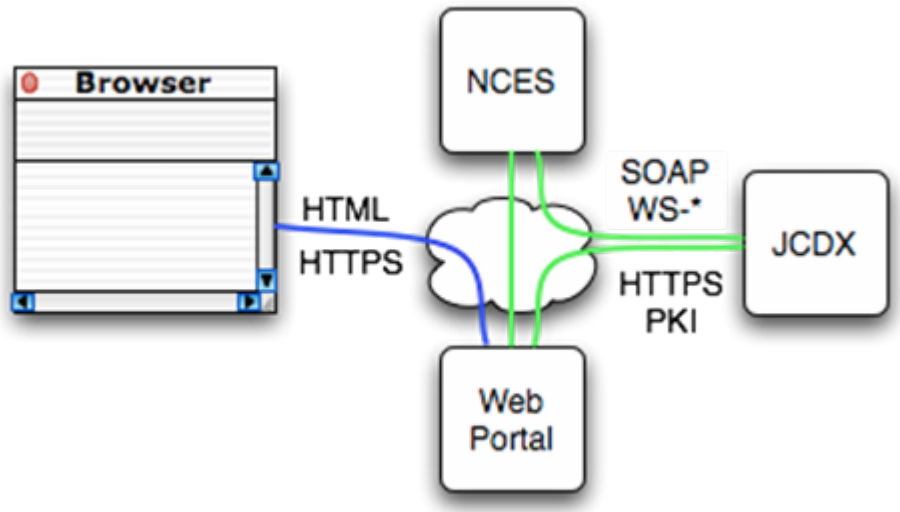


JCDX Web Services

- Classification Policy Decision Service (cPDS)
  - provides other systems with methods for handling labeled data such as label comparison
- Federated Search Provider
  - allows users and applications to search multi-level data stores from single level networks and provides a “read down” capability to all lower level domains

cPDS clearance based authentication

- Current NCES Security Services only implements role based access control
- First attempt to authorize the user via NCES RBAC, and then attempt to authorize the user's clearance via JCDX cPDS



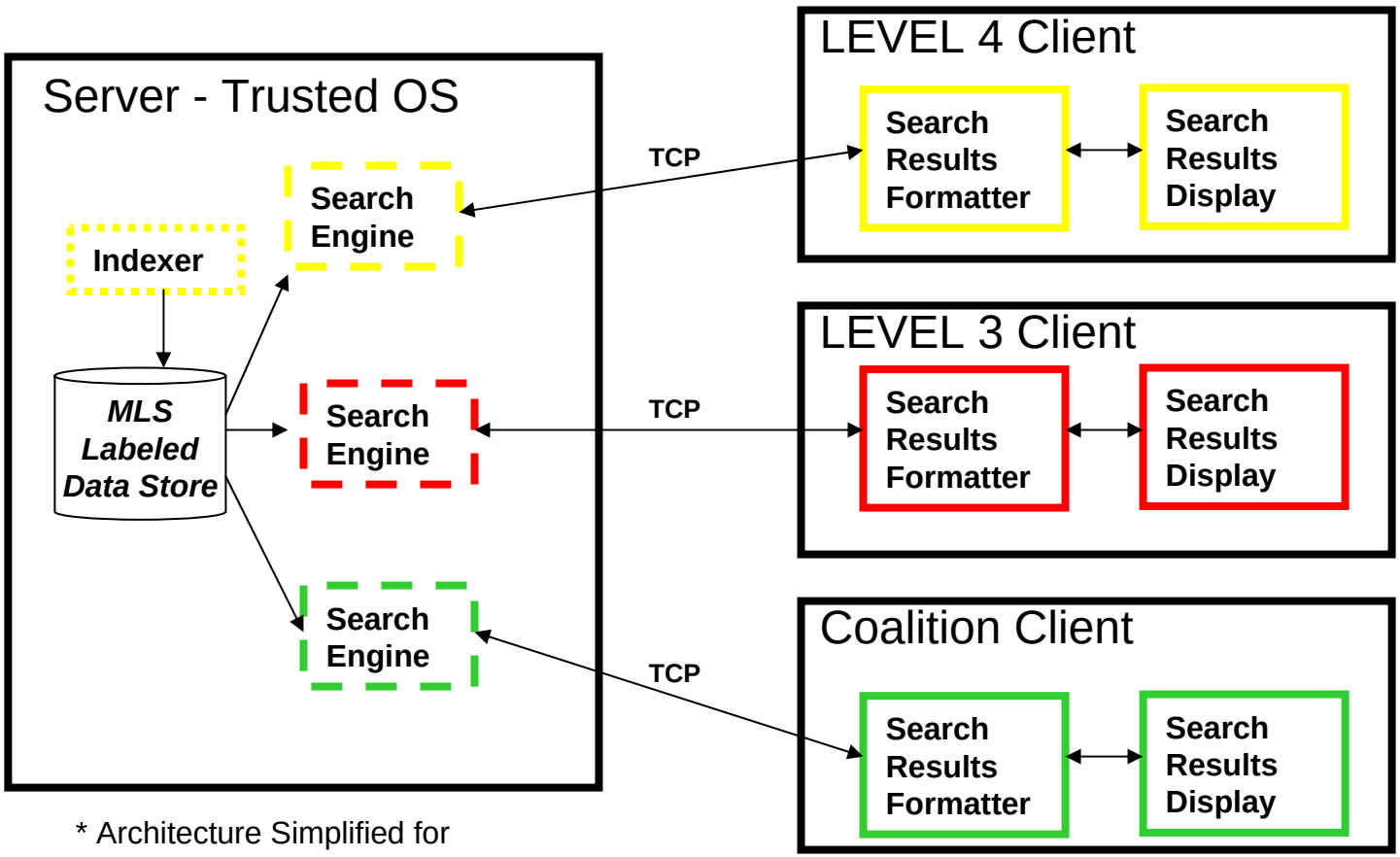
Other cPDS methods

- **isValid:** takes a classification and returns whether the classification is valid
- **getRelationship:** takes two arguments, a Subject Clearance and an Object Classification and returns the relationship. The relationship can be one of the following: Subject Strictly Dominates, Equal, Object Strictly Dominates, and Incomparable
- **getAggregateClassifcation:** takes a list of classifications and produces a classification that is the 'sum' of the arguments. (e.g. *getAggregateClassification* 'SECRET REL GBR' 'SECRET' 'UNCLASSIFIED' yields 'SECRET').
- **getGroupClearance:** takes a list of user clearances and produces a group clearance. This group clearance is the highest classification that can be read by all of the users in the group
- **iSReleasableTo:** takes a data classification and a list of clearances and determines whether the data can be released to all of the users whose clearances were used as arguments
- **canReceive:** The *canReceive* method takes a user clearance and a list of data classifications and determines whether the user can see all of the data whose classifications were used as arguments

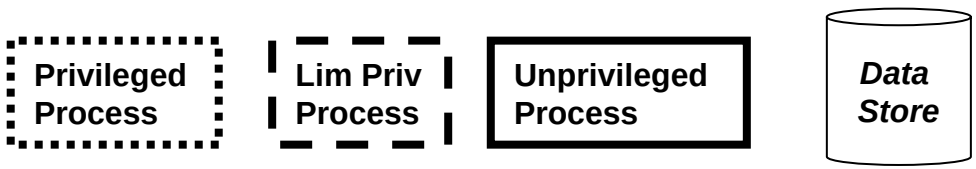
Federated Search Provider

- Allows searching of the JCDX MLS PL4 data repository through a Web Service
- Authenticates the search request via NCES and cPDS and then returns messages at the appropriate classification (including “read-down”)

Applying JCDX Design Approach to Achieve Enterprise Wide CDS Capability



* Architecture Simplified for Illustrative Purposes



Other Critical Pieces (Future Work)

- Trusted Editor
- Trust Service
- Labeling Service
- Accreditation / Policy Changes

Trusted Editor

- Content producers need a method to produce labeled content
  - Must be able to “trust” the label
- Unreasonable to expect all users to have MLS clients
  - Microsoft Windows has a very low “trust” level

Trust Service

- Transferring labeled data between two **systems** must involve a trusted interaction
- In non-SOA these trust relationships are statically defined
- SOA needs an automated method to determine which services on the network are trusted
- Trust service could be queried to determine the level of trust that a given service/system has

Labeling Service

- Must be able to transition unlabeled content in to labeled content
- Labeling service would provide an interface to allow the submission of content for labeling
  - assign a security label to the content based on a pre-defined ruleset
  - then “sign” the associated label to allow other services to verify the given label

Summary

- JCDX has begun to bridge the gap between traditional MLS systems and SOA and has developed an architecture that can be applied to other MLS systems
- JCDX Web Service Gateway's can be used to extend MLS capabilities to single level clients
- Extending MLS systems to a SOA enables coalition operations

Points of Contact

PEO C4I PMW160	CDR Wayne Slocum	619-524-7511	Wayne.slocum@navy.mil
PEO C4I PMW160 APM	Maureen Myer	619-553-9748	Penney.myer@navy.mil
PEO C4I PMW160 Chief Engineer	Robert Fish	619-553-6406	Robert.fish@navy.mil
JCDX Chief Engineer	Paul Kennedy	619-553-9541	Paul.kennedy@navy.mil
JCDX Chief Scientist	Chris J. Raney	619-553-5282	raneyc@spawar.navy.mil
PEO C4I FMS Case Manager	Steve Reddick	619-524-7274	Steven.reddick@navy.mil